

Appendix A

```
<SigningRequest Return="Signature">
  <Policy>
    <SignatureInfo Type="detached"/>
    <KeyInfo>
      <KeyName
Type="email_name">rsalz@zolera.com</KeyName>
      </KeyInfo>
      <CertChain Length="All" Type="Certificate"/>
    </Policy>
    <Document URI="url of document" />
  </SigningRequest>
```

Appendix B

```
<SigningRequest>
  <Policy>
    <SignatureInfo Type="enveloped"/>
    <KeyInfo>
      <X509Data>
        <X509IssuerSerial>
          <X509IssuerName>CN=Rich Salz, O=Zolera, C=US
          </X509IssuerName>
          <X509SerialNumber>12345678</X509SerialNumber>
        </X509IssuerSerial>
      </X509Data>
    </KeyInfo>
    <CertChain Length="All" Type="Certificate"/>
  </Policy>
  <Document URI="url of document"
Algorithm="http://www.w3.org/2000/09/xmlsig#base64">
    base64 encoded document
  </Document>
</SigningRequest>
```

Appendix C

```
<purchaseOrder orderDate="1999-10-20">
  <items>
    <item partNum="872-AA">
      <productName>Lawnmower</productName>
      <quantity>1</quantity>
      <USPrice>148.95</USPrice>
    </item>
  </items>
</purchaseOrder>
```

Appendix D

```
<SigningRequest Return="Signature">
  <Policy>
    <SignatureInfo Type="enveloped"/>
    <KeyInfo>
      <KeyName
Type="email_name">rsalz@zolera.com</KeyName>
      </KeyInfo>
      <CertChain Length="None"/>
    </Policy>
    <Document URI="po_txn_123">
      <purchaseOrder orderDate="1999-10-20">
        <items>
          <item partNum="872-AA">
            <productName>Lawnmower</productName>
            <quantity>1</quantity>
            <USPrice>148.95</USPrice>
          </item>
        </items>
      </purchaseOrder>
    </Document>
  </SigningRequest>
```

Appendix E

```
<purchaseOrder orderDate="1999-10-20">
  <items>
    <item partNum="872-AA">
      <productName>Lawnmower</productName>
      <quantity>1</quantity>
      <USPrice>148.95</USPrice>
    </item>
  </items>
  <Signature Id="178ae4" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <SignatureMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">

        <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
        </Reference>
        <Reference
URI="#ServerSignatureProperties"Type="http://www.w3.org/2000/09/xm
ldsig#SignatureProperty">
        <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>k3453rvEPO0vKtMup4NbeVu8nk=</DigestValue>
        </Reference>
        <Reference URI="#KeyInfo">
        <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>7abc3rvEPO0vKtMupdefVxdu8nk=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
      <KeyInfo Id="KeyInfo">
        <KeyNameType="email_name">rsalz@zolera.com</KeyName>
      </KeyInfo>
    </Object>
    <SignatureProperties>
      <SignaturePropertyId="ServerSignatureProperties">
        <ServerInfoxmlns="urn:caveosystems:sign1">
          <ServerIdentifier>hancock serveridentifier</ServerIdentifier>
        </ServerInfo>
      </SignatureProperty>
    </SignatureProperties>
  </Signature>
  <SignatureReference>AB14E72
</SignatureReference>

  <AuthenticityStamp>blob</AuthenticityStamp>
  <VerificationURI>http://www.zolera.com/2000/VerifierService/
</VerificationURI>
</ServerInfo>
  <timestamp xmlns="http://www.ietf.org/rfcXXXX.txt">YYYYMMDDHHMMSS.fffz
</timestamp>
</SignatureProperty>
</SignatureProperties>
</Object>
</Signature>
</purchaseOrder>
```

Appendix F

```

<SigningResponse>
  <Status Type="Success"/>
  <SignatureResult Return="Signature">
    <Signature Id="178ae4" xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <Reference URI="">
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>j6lwx3rvEP00vKtMup4NbeVu8nk=</DigestValue>
            </Reference>
          <Reference
URI="#ServerSignatureProperties"Type="http://www.w3.org/2000
/09/xmldsig#SignatureProperty">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>k3453rvEP00vKtMup4NbeVu8nk=</DigestValue>
            </Reference>
          <Reference URI="#KeyInfo">
            <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>7abc3rvEP00vKtMupdefVxdu8nk=
            </DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
        <KeyInfo Id="KeyInfo">
          <KeyName Type="email_name">rsalz@zolera.com</KeyName>
        </KeyInfo>
      </Object>
    <SignatureProperties>
      <SignatureProperty Id="ServerSignatureProperties"
xmlns="urn:caveosystems:sign1">
        <ServerInfo
server identifier</ServerIdentifier>
          <SignatureReference>AB14E72
        </SignatureReference>
        <AuthenticityStamp>blob</AuthenticityStamp>
      </SignatureProperty>
    </SignatureProperties>
  </Object>
</Signature>
</SignatureResult>
</SigningResponse>
<VerificationURI>http://www.zolera.com/2000/VerifierService/</VerificationURI>
  </ServerInfo>
  <timestamp xmlns="http://www.ietf.org/rfcXXXX.txt">
    YYYYMMDDHHMMSS.fffZ</timestamp>
</SignatureProperty>
</SignatureProperties>
</Object>
</Signature>
</SignatureResult>
</SigningResponse>

```

Appendix G

```
<VerificationRequest Type="receipt">
  <VerifyInfo>
    <Signature>
      The XML signature to be verified, including
      SignedInfo and Objects. Hancock Signature Object and
      KeyInfo required.
    </Signature>

    <Document URI="url of document"
      Algorithm="http://www.w3.org/2000/09/xmldsig#base64">
      base64 encoded document
    </Document>
  </VerifyInfo>
</VerificationRequest>
```

Appendix H

```
<VerificationRequest>
  <VerifyInfo>
    <Signature Id="7"/>
    <Document
      URI="http://www.zolera.com/example.xml"/>
    </VerifyInfo>
</VerificationRequest>
```

Appendix I

```
<VerificationResponse>
  <VerifyInfo>
    <SignatureReference Type="Id">7</SignatureReference>
    <SignatureStatus Type="Invalid"/>
    <CredentialStatus Type="Revoked"
      Type="Certificate">MIICPzCCA...</CredentialStatus>
    </VerifyInfo>
    <ServerIdentifier>75axxx</ServerIdentifier>
    <Timestamp></Timestamp>
  </VerificationResponse>
```

Appendix J

```
<VerificationResponse TYPE="receipt">
  elements as defined above, and additional Signature
  elements:
    <Signature>
      <SignedInfo </SignedInfo>
      <Object>
        <SignatureProperties>
          <SignatureProperty
            Id="ServerSignatureProperties"> as defined above
          </SignatureProperty>
        </SignatureProperties>
      </Object>
    </Signature> </VerificationResponse>
```

Appendix K

```
<SignatureSummaryRequest>
  <SignedDocument URI="url of document"
  Algorithm="http://www.w3.org/2000/09/xmlsig#base64">
    base64 encoded document
  </SignedDocument>
</SignatureSummaryRequest>
```

Appendix L

```
<SignatureSummaryRequest>
  <SignedDocumentIdentifier
>7E5</SignedDocumentIdentifier>
  <SignatureIdentification Id="78"/>
</SignatureSummaryRequest>SignedDocumentIdentifier
```

Appendix M

```
<SignatureSummary >
  <SignatureInfo Id="firstsig" TYPE="detached">
    <KeySummary Length="56" Rating="B"/>
    <SignatureSummary
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
Rating="C+"/>
    <CredentialSummary Type="none" Rating="F"/>
  <SignatureInfo>
    <SignatureInfo Id="secondsig" TYPE="enveloped">
      <KeySummary Length="128" Rating="A"/>
      <SigSummary
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
Rating="A"/>
      <CredentialSummary Type="x509" Rating="c">
        <X509Data> <!-- certificate chain -->
          <!--Signer cert, issuer
C=US,O=IBM,OU=FVT,CN=arbolCA serial 4-->
          <X509Certificate>MIICXTCCA...</X509Certificate>
          <!-- Intermediate cert subject
C=US,O=IBM,OU=FVT,CN=arbolCAissuer,C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
          <X509Certificate>MIICPzCCA...</X509Certificate>
          <!-- Root cert subject
C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
          <X509Certificate>MIICSTCCA...</X509Certificate>
          <!-- Root cert subject
C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
          <X509Certificate>MIICSTCCA...</X509Certificate>
        </X509Data>
      </CredentialSummary>
    <SignatureInfo>
      <Disclaimer>text</Disclaimer>
    </SignatureSummary>
```

Tested by [illegible]

	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	2101	2102	2103	2104	2105	2106	2107	2108	2109	2110	2111	2112	2113	2114	2115	2116	2117	2118	2119	2120	2121	2122	2123	2124	2125	2126	2127	2128	2129	2130	2131	2132	2133	2134	2135	2136	2137	2138	2139	2140	2141	2142	2143	2144	2145	2146	2147	2148	2149	2150	2151	2152	2153	2154	2155	2156	2157	2158	2159	2160	2161	2162	2163	2164	2165	2166	2167	2168	2169	2170	2171	2172	2173	2174	2175	2176	2177	2178	2179	2180	2181	2182	2183	2184	2185	2186	2187	2188	2189	2190	2191	2192	2193	2194	2195	2196	2197	2198	2199	2200	2201	2202	2203	2204	2205	2206	2207	2208	2209	2210	2211	2212	2213	2214	2215	2216	2217	2218	2219	2220	2221	2222	2223	2224	2225	2226	2227	2228	2229	2230	2231	2232	2233	2234	2235	2236	2237	2238	2239	2240	2241	2242	2243	2244	2245	2246	2247	2248	2249	2250	2251	2252	2253	2254	2255	2256	2257	2258	2259	2260	2261	2262	2263	2264	2265	2266	2267	2268	2269	2270	2271	2272	2273	2274	2275	2276	2277	2278	2279	2280	2281	2282	2283	2284	2285	2286	2287	2288	2289	2290	2291	2292	2293	2294	2295	2296	2297	2298	2299	2300	2301	2302	2303	2304	2305	2306	2307	2308	2309	2310	2311	2312	2313	2314	2315	2316	2317	2318	2319	2320	2321	2322	2323	2324	2325	2326	2327	2328	2329	2330	2331	2332	2333	2334	2335	2336	2337	2338	2339	2340	2341	2342	2343	2344	2345	2346	2347	2348	2349	2350	2351	2352	2353	2354	2355	2356	2357	2358	2359	2360	2361	2362	2363	2364	2365	2366	2367	2368	2369	2370	2371	2372	2373	2374	2375	2376	2377	2378	2379	2380	2381	2382	2383	2384	2385	2386	2387	2388	2389	2390	2391	2392	2393	2394	2395	2396	2397	2398	2399	2400	2401	2402	2403	2404	2405	2406	2407	2408	2409	2410	2411	2412	2413	2414	2415	2416	2417	2418	2419	2420	2421	2422	2
--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	---

</Signature>

Appendix P

</Reference>

</KeyInfo>

Appendix Q

```
<Object>
  <SignatureProperties>
    <SignatureProperty Id="ServerSignatureProperties">
      <HancockSignatureProperties></HancockSignatureProperties>
    </SignatureProperty>
  </SignatureProperties>
</Object>
```

Appendix R

```
<Reference URI="#ServerSignatureProperties"
Type="http://www.w3.org/2000/09/xmldsig#SignatureProperty">
  <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>k3453rvEP00vKtMup4NbeVu8nk=</DigestValue>
  </Reference>
```

Appendix S

```
POST /SigningRequest HTTP/1.1
Host: www.signingserver.com
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: "Some-URI"

<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/en
coding/">
  <SOAP-ENV:Body>
    <SigningRequest Return="Signature"
xmlns:"urn:caveosystems:sign1">
      <Policy>
        <SignatureInfo Type="detached"/>
        <KeyInfo>
          <KeyName
Type="email_name">rsalz@zolera.com</KeyName>
          </KeyInfo>
          <CertChain Length="All" Type="Certificate"/>
        </Policy>
        <Document URI="url of document" />
      </SigningRequest>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

TESTING - 2004-04-05